Process Safety Beacon
Messages for Manufacturing Personnel
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

This issue sponsored by
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

امنیت سایبری و بهره برداری در صنایع شیمیایی

جولای ۲۰۲۱

آیا می دانستید؟

- مجرمان اینترنتی برای رسیدن به اهداف خود از بدافزارهای پیشرفته در نقاط آسیب پذیر استفاده می کنند.
- حملات باج خواهی به عنوان ابزاری برای درآمد زایی و کسب پول بصورت سازمان یافته در حال افزایش است.
- بر اساس مطالعات اخیر هر ۳۹ ثانیه یک حمله سایبری اتفاق می افتد.

(Ref. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)

- فیشینگ (Phishing) یا ارسال ایمیل روشی است که فرد در ظاهراً از شرکت های معتبر ایمیلی دریافت کرده و ترغیب می شود تا اطلاعات شخصی خود را افشا کند. این متد یکی از معمول ترین روش های ورود بدافزار است.
- تهدیدات سایبری می توانند از طریق ایمیل ها، پیوست ها و یا تجهیزات ذخیره سازی قابل حمل اطلاعات، مانند درایوهای USB یا سایر وسایل ذخیره سازی قابل حمل به سیستم های نرم افزاری شرکت وارد شوند.
- در نود و پنج درصد از موارد، نادیده گرفتن و نقض امنیت سایبری به دلیل خطای انسانی است.

(Ref. https://www.cybintsolutions.com/employee-education-reduces-risk/)

شما چه کاری می توانید انجام دهید؟

- همواره قبل از بروز نمودن نرم افزار، تائیدیه لازم از واحد IT اخذ کرده و سپس در زمان مناسب و بموقع نسخهٔ تائید شده را نصب نمائید.
- از بروز بودن و روشن بودن فایروال ها (Firewalls) و سایر نرم افزارهای شبکه اطمینان حاصل کنید.
- اطمینان حاصل نمائید که به طور منظم از سیستم ها و داده های خود نسخه پشتیبان تهیه می شود.
- برای تمام دسترسی های خود از رمزهای عبور (Passwords) مناسب و قوی استفاده کنید. رمزهای عبورِ حساب کاربری خود را در اختیار هیچ کس قرار نداده و به طور مرتب رمزهای عبور را تغییر دهید.
- رمزهای عبور خود را در مرورگرها (Browsers) ذخیره نکنید.
- بر روی لینک ها و یا پیوست ها در ایمیل هایی که از افراد ناشناس دریافت می کنید، کلیک نکنید.
- هرگز نرم افزار تأیید نشده ای را بر روی هیچ یک از کامپیوتر های شرکت نصب نکنید. اطمینان یابید که صفحه کلید و سایر تجهیزات حفاظتی، امنیت سیستم را به خوبی تامین می کنند.
- اگر بصورت دسترسی از راه دور کار می کنید، الزامات سازمان را اجرا کنید. بخصوص اگر از مکان های دسترسی اینترنت عمومی استفاده می کنید بسیار مراقب باشید.
- اگر در کامپیوترتان با موردی عجیب و متفاوت مواجه شدید، درخواست کمک کنید. ممکن است هکری در حال تلاش جهت دسترسی به کامپیوتر شما باشد.

شکل ۱: واحد تصفیه خانه آب در Oldsmar، فلوریدا

در تاریخ ۵ فوریه ۲۰۲۱، کارمندی در تصفیه خانه Oldsmar، فلوریدا متوجه شد که مکان نما به طور عجیبی بر روی صفحه نمایش کنترل کامپیوتر حرکت می کند. در ابتدا هیچ نگرانی وجود نداشت چون این واحد از نرم افزار دسترسی از راه دور (Remote Access) استفاده می کرد تا کارکنان امکان به اشتراک گذاری صفحات نمایش و رفع مشکلات IT را داشته باشند. سرپرستِ واحد معمولا به کامپیوتر اپراتور متصل میشد تا سیستم های تأسیسات را پایش کند. چند ساعت بعد، اپراتور متوجه شد که مکان نما روی صفحه کنترل حرکت کرده و کلیک هایی انجام می شود. در عرض چند ثانیه، متجاوز تلاش می کرد تا سیستم تنظیم هیدروکسید سدیم را از ۱۰۰(ppm) به ۱۱۱۰۰ (ppm) تغییر دهد. اپراتور خیلی سریع متوجه نفوذ شد و میزان هیدروکسید سدیم را به سطح نرمال بازگرداند. خوشبختانه، این موضوع تاثیری در کیفیت آب نداشت.

حمله اخیرِ باج خواهی به خط لوله کلونیال (Colonial Pipeline) عرضهٔ بنزین به سواحل شرقیِ ایالات متحده را برای چندین روز متوقف کرد.

احتمالا سیستم های شرکت شما نیز به اینترنت متصل اند و به محافظت در برابر تهدیدات سایبری نیاز دارند. استراتژی های زیادی توسط شرکت ها برای جلوگیری از تهدیدات سایبری استفاده می شوند مانند: فایروال ها (Firewalls)، نرم افزارهای ضد ویروس و سیاست های محافظت در برابر بدافزار و ویروس های رایانه ای.

هم اکنون افراد زیادی از راه دور کار می کنند، به همین دلیل امکان حملات سایبری به مراتب افزایش یافته است.

حملات سایبری واقعی هستند. برای دفاع از آن شما نقشی حیاتی دارید.

M. Sattarghour